

REMARKS

This Application has been reviewed in light of the Office Action dated April 21, 2006.

Claims 1-15, 45, and 46 are presented for examination. Claims 1, 6, 9, 12, and 13 have been amended to define more clearly what Applicants regard as their invention. Claims 1, 6, 9, 12, and 13 are in independent form. Favorable reconsideration is requested.

Applicants note that three of the four documents cited in the Information Disclosure Statement dated May 2, 2002, were initialed on the form PTO-1449; to ensure that the record is clear, and that all four documents are listed on the face of any patent that may issue from this application, Applicants respectfully request that the fourth listed document also be initialed to confirm that the Examiner has considered it. Also, Applicants note that a further Information Disclosure Statement was filed on April 20, 2006, and ask that the Examiner, in due course, consider and make of record the documents cited therein.

Claims 1, 3-5, 6, 9, 11-13, and 15 were rejected under 35 U.S.C. § 102(b) as being anticipated by Japanese Patent Application Laid-Open No. JPA 09-244828 (*Akihiko*). Claims 2, 7, 10, and 14 were rejected under 35 U.S.C. § 103(a) as being obvious from *Akihiko* in view of Japanese Patent Application No. JPA 07-073128 (*Takeshi*).

The present invention relates to controlling a printer to generate and print a plurality of print jobs as a single combined print job when appropriate permission is obtained, for example, when the user is authenticated. When such permission is not obtained, the print job is not generated, and an indication that such permission was not obtained is transmitted to a job accounting application.

For example, independent Claim 1 is directed to a print control apparatus for performing user authentication processing in print processing including a job combination unit, a request unit, and a transmission control unit. The job combination unit combines a plurality of print jobs into a single combined print job. The request unit issues a request, including an input user ID, to an authentication server

for obtaining permission to print the single combined print job. The transmission control unit includes a printer driver for controlling a process so that, when permission is obtained from the authentication server, print data based upon the single combined print job is generated and transmitted to a printer. When permission is not obtained (i) the print data based upon the single combined print job is not generated and (ii) an indication that permission was not obtained from the authentication server is transmitted to a job accounting application by the printer driver.

By virtue of the features of the apparatus of Claim 1, when a user is authenticated, a single combined print job is generated and transmitted to a printer. When that is not the case, the print job is not generated, thus avoiding the waste of time and processing on the generation of print data that will not be used, and an indication that the user was not authenticated is transmitted to a job accounting application.

Thus, an efficient print control apparatus is provided because print data is not generated by a printer driver when a user is not authenticated.

Applicants submit that *Akihiko* relates to a security system for a printer wherein a secret document is generated and transmitted from a host computer to the printer and is stored in a HDD of the printer. The printer informs the host computer of a job number assigned to the stored document via a print server, and the previously generated and stored secret document is printed when a user is authenticated by inputting a pre-registered password and the job number assigned to the secret document. When the user is not authenticated, the previously generated and stored document is erased.

In the *Akihiko* system, a secret document is generated and transmitted from a host to a printer and stored in the printer even when the user is not authenticated. However, in the apparatus of Claim 1, a print job is not generated when the user is not authenticated.

Further, in the *Akihiko* system, in contradistinction to the apparatus of Claim 1, no indication that permission was denied by the authentication server is transmitted.

Accordingly, Claim 1 is seen to be clearly allowable over *Akihiko*.

Independent Claims 6, 9, 12 and 13 are directed to a method, storage medium, program, and system, respectively, corresponding to the apparatus recited in Claim 1, and are also believed to be patentable over *Akihiko* for at least the same reasons.

A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as a reference against the independent claims herein. Those claims are, therefore, believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Leonard P Diana/
Leonard P. Diana
Attorney for Applicants
Registration No. 29,296

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200